

Before the
Federal Communications Commission
Washington, D.C. 20554

RECEIVED

DEC 14 1998

FEDERAL COMMUNICATIONS COMMISSION
OFFICE OF THE SECRETARY

In the Matter of:)
)
Communications Assistance for) CC Docket No. 97-213
Law Enforcement Act)

COMMENTS OF METRICOM, INC.

Metricom, Inc. ("Metricom"), by its attorneys, pursuant to Section 1.415 of the Commission's rules, hereby submits its comments in response to the Further Notice of Proposed Rule Making in the above-captioned proceeding ("*Further Notice*").¹

I. Introduction

Metricom is a young, rapidly growing, technologically innovative company based in Silicon Valley. Metricom has developed devices operating under Part 15 of the Commission's rules that enable it to offer a wireless data and information service called Ricochet™ using a combination of its wireless packet-mode data network and its high-speed frame relay network of leased lines. While Metricom's information service is exempt from the assistance capability requirements of CALEA,²

-
1. Communications Assistance for Law Enforcement Act, *Further Notice of Proposed Rule Making*, FCC 98-282 (rel. Nov. 5, 1998).
 2. See Section 103(b)(2)(A) (exempting information services from assistance requirements).

0014024.01

No. of Copies rec'd 014
List ABCDE

Metricom remains an interested party to the extent that it may be deemed by the Commission to be a “telecommunications carrier” as that term is defined in CALEA.³

Metricom’s comments are directed to that portion of the *Further Notice* in which the Commission solicits comment on how CALEA’s assistance requirements should apply to packet mode telecommunications.⁴

II. Analysis

If the Commission, after consideration of the record in this proceeding, imposes technical requirements for packet-mode telecommunications, those requirements must comply with section 107(b) of CALEA.⁵ That section requires, *inter alia*, that technical standards must “meet the assistance capability requirements of Section 103 *by cost effective methods*.”⁶ Metricom questions whether *any* technical standards that are directed at interception of the content of wireless packet-mode telecommunications can satisfy the requirement that the methods used be cost-effective. The reason is that wireless data carriers typically provide their customers with strong encryption that makes meaningful interception of call content impossible.⁷ Therefore, as to these carriers, any costs

3. See Section 102(8), 47 U.S.C. § 1001(8). That definition includes entities engaged in providing commercial mobile service as well as those providing switching or transmission service “to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service.” *Id.*

4. *Further Notice* at ¶¶ 58-66.

5. 47 U.S.C. § 1006(b).

6. Section 107(b)(1), 47 U.S.C. § 1006(b)(1) (emphasis added).

7. “Strong encryption” refers to an encryption system that is essentially unbreakable, under
(continued...)

incurred in complying with CALEA's call-content interception requirements are not effective in delivering useful information to law enforcement agencies (LEAs).

The assistance requirements of CALEA are intended to enable LEAs to gain access to the content of a subscriber's communications⁸ and to the call-identifying information associated with such a communication.⁹ However, Congress tempered LEAs' rights to gain access to this information by a reasonableness requirement. Thus, any standards adopted by the Commission must, as quoted above, meet LEA objectives through "cost effective methods." Similarly, as reported by Congress, CALEA is intended to "excuse a failure to comply with the assistance capability requirements or capacity notices where the cost of compliance is wholly out of proportion to the usefulness of achieving compliance for a particular type or category of services or features."¹⁰

For the category of wireless data communications services, the usefulness of achieving compliance with the content interception requirements is practically nil. Metricom, like other wireless information service providers, offers its subscribers strong encryption which Metricom has no ability to decrypt. Although the spread-spectrum technology employed by Metricom makes its wireless transmissions difficult to intercept, wireless signals generally are easier for unintended parties to intercept than wireline signals. Consequently, customers choosing to transmit information over wireless facilities *demand* the security provided by strong encryption. CALEA does not require

7. (...continued)
current technology, without access to the decryption key. *See, e.g.,*
<http://www.whatis.com/encrypti.htm> (visited Dec. 12. 1998).

8. Section 103(a)(1), 47 U.S.C. § 1002(a)(1).

9. Section 103(a)(2), 47 U.S.C. § 1002(a)(2).

10. H.R. Rep. No. 103-827 at 28 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3508.

that carriers provide LEAs with the ability to decrypt user-encrypted communications.¹¹ Therefore, since strong encryption is virtually unbreakable, the content of communications intercepted from a wireless data communications service is virtually worthless to a LEA.

Because intercepted wireless packet-mode data content information is virtually worthless, the costs to wireless data communications service providers of complying with packet-mode call-content interception requirements, not to mention the costs to society of developing technical standards for packet-mode call-content interceptions, cannot be justified no matter how small (and Metricom believes that the costs are substantial).

III. Conclusion

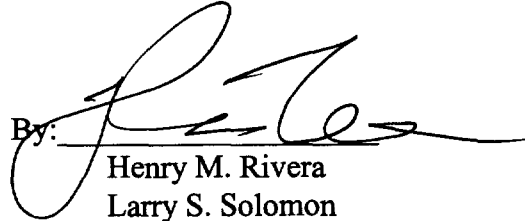
Since the content of encrypted wireless packet-mode data transmissions is virtually worthless to LEAs, while the costs of implementing the assistance capabilities of CALEA for such transmissions are likely to be substantial, technical standards that would require wireless packet-mode data carriers to provide *any* call content information are not cost effective. Accordingly, technical standards for wireless packet-mode data carriers to comply with the assistance capabilities

11. See Section 103(b)(3), 47 U.S.C. § 1002(b)(3) (“A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.”).

of CALEA should require those carriers to provide, at most, call-identifying information that is reasonably available to the carrier, but no call-content information.

Respectfully submitted,

METRICOM, INC.

By: 

Henry M. Rivera
Larry S. Solomon
J. Thomas Nolan
SHOOK, HARDY & BACON L.L.P.
1850 K Street, NW
Suite 900
Washington, DC 20006
(202) 452-1450

Its attorneys

Dated: December 14, 1998